Isotopic classes of Transversals

Vipul Kakkar* and R.P. Shukla
Department of Mathematics, University of Allahabad
Allahabad (India) 211 002
Email: vplkakkar@gmail.com; shuklarp@gmail.com

Abstract

Let G be a finite group and H be a subgroup of G. In this paper, we prove that if G is a finite nilpotent group and H a subgroup of G, then H is normal in G if and only if all normalized right transversals of H in G are isotopic, where the isotopism classes are formed with respect to induced right loop structures. We have also determined the number isotopy classes of transversals of a subgroup of order 2 in D_{2p}, the dihedral group of order $2p$, where p is an odd prime.

classification: 20D60; 20N05
keywords: Right loop, Normalized Right Transversal, Isotopy

1 Introduction

Let G be a group and H be a subgroup of G. A *normalized right transversal (NRT)* S of H in G is a subset of G obtained by choosing one and only one element from each right coset of H in G and $1 \in S$. Then S has a induced binary operation $\circ$ given by $\{x \circ y\} = Hxy \cap S$, with respect to which S is a right loop with identity 1, that is, a right quasigroup with both sided identity (see [11, Proposition 4.3.3, p.102],[8]). Conversely, every right loop can be embedded as an NRT in a group with some universal property (see [8, Theorem 3.4, p.76]). Let $\langle S \rangle$ be the subgroup of G generated by S and H_S be the subgroup $\langle S \rangle \cap H$. Then $H_S = \langle \{xy(x \circ y)^{-1} | x, y \in S\} \rangle$ and $H_S S = \langle S \rangle$

*The first author is supported by CSIR, Government of India.

(see [8]). Identifying S with the set $H\backslash G$ of all right cosets of H in G, we get a transitive permutation representation $\chi_S : G \rightarrow Sym(S)$ defined by $\{\chi_S(g)(x)\} = Hxg \cap S, g \in G, x \in S$. The kernal $Ker\chi_S$ of this action is $Core_G(H)$, the core of H in G.

Let $G_S = \chi_S(H_S)$. This group is known as the *group torsion* of the right loop S (see [8, Definition 3.1, p.75]). The group G_S depends only on the right loop structure $\circ$ on S and not on the subgroup H. Since χ_S is injective on S and if we identify S with $\chi_S(S)$, then $\chi_S(\langle S\rangle) = G_S S$ which also depends only on the right loop S and S is an NRT of G_S in $G_S S$. One can also verify that $Ker(\chi_S|_{H_S S} : H_S S \rightarrow G_S S) = Ker(\chi_S|_{H_S} : H_S \rightarrow G_S) = Core_{H_S S}(H_S)$ and $\chi_S|_S$=the identity map on S. Also $(S, \circ)$ is a group if and only if G_S trivial.

Two groupoids $(S, \circ)$ and $(S', \circ')$ are said to be *isotopic* if there exists a triple (α, β, γ) of bijective maps from S to S' such that $\alpha(x) \circ' \beta(x) = \gamma(x \circ y)$. Such a triple (α, β, γ) is known as an isotopism or isotopy between $(S, \circ)$ and $(S', \circ')$. We note that if (α, β, γ) is an isotopy between $(S, \circ)$ and $(S', \circ')$ and if $\alpha = \beta = \gamma$, then it is an isomorphism. An *autotopy*(resp. *automorphism*) on S is an isotopy (resp. isomorphism) form S to itself. Let $\mathcal{U}(S)$(resp. $Aut(S)$) denote the group of all aututopies (resp. automorphisms) on S. Two groupoids $(S, \circ)$ and $(S, \circ')$, defined on same set S, are said to be *principal isotopes* if (α, β, I) is an isotopy between $(S, \circ)$ and $(S, \circ')$, where I is the identity map on S (see [2, p. 248]). Let $\mathcal{T}(G, H)$ denote the set of all normalized right transverslas (NRTs) of H in G. In next section, we will investigate the isotopism property in $\mathcal{T}(G, H)$. We say that $S, T \in \mathcal{T}(G, H)$ are isotopic, if their induced right loop structures are isotopic. Let $\mathcal{I}tp(G, H)$ denote the set of isotopism classes of NRTs of H in G. If $H \trianglelefteq G$, then each NRT $S \in \mathcal{T}(G, H)$ is isomorphic to the quoteint group G/H. Thus $|\mathcal{I}tp(G, H)| = 1$. We feel that the converse of the above statement should also be true. In next section, we will prove that if G is a finite nilpotent group and $|\mathcal{I}tp(G, H)| = 1$, then $H \trianglelefteq G$.

In sections 2 and 3, we discuss isotopy classes of transversals in some particular groups. The main results of section 3 are Proposition 2.8 and Theorem 2.14. The main results of Section 4 are Theorem 3.7 and Theorem 3.9, which describe the isotopy classes of transversals of a subgroup of order 2 in D_{2p}, the dihedral group of order $2p$, where p is an odd prime.

2 Isotopy in $\mathcal{T}(G, H)$

Let $(S, \circ)$ be a right loop. For $x \in S$, we denote the map $y \mapsto y \circ x$ $(y \in S)$ by R°_x. Let $a \in S$ such that the equation $a \circ X = c$ has unique solution for all $c \in S$, in notation we write it as $X = a \backslash_{\circ} c$. Then the map $L^{\circ}_a : S \to S$ defined by $L^{\circ}_a(x) = a \circ x$ is bijective map. Such an element a is called a *left non-singular* element of S. We will drop the superscript, if the binary operation is clear. It is observed in [2, Theorem 1A, p.249] that $(S, \circ')$ is a principal isotope of $(S, \circ)$, where $x \circ' y = (R^{\circ}_b)^{-1}(x) \circ (L^{\circ}_a)^{-1}(y)$ under the isotopy $((R^{\circ}_b)^{-1}, (L^{\circ}_a)^{-1}, I)$ from $(S, \circ')$ to $(S, \circ)$ and every principal isotope is of this form. Let us denote this isotope by $S_{a,b}$. It is also observed in [2, Lemma 1A, p.248] that if right loop $(S_1, \circ_1)$ is isotopic to the right loop $(S_2, \circ_2)$, then $(S_2, \circ_2)$ is isomorphic to $(S_1, \circ')$, the principal isotope of $(S_1, \circ_1)$ defined above. Write the equation $x \circ' y = (R^{\circ}_b)^{-1}(x) \circ (L^{\circ}_a)^{-1}(y)$ by $R^{\circ'}_y(x) = R^{\circ}_{(L^{\circ}_a)^{-1}(y)}((R^{\circ}_b)^{-1}(x))$. This means that if S_1 and S_2 are isotopic right loops, then $G_{S_1}S_1 \cong G_{S_2}S_2$.

Proposition 2.1. *Let $(S, \circ)$ and $(S', \circ')$ be isotopic right loops. Then the set of left non-singular elements of S is in bijective correspondence to that of S'.*

Proof. Let (α, β, γ) be an isotopy from $(S, \circ)$ to $(S', \circ')$. Let $a \in S$ such that $\alpha(a)$ is a left non-singular element of S'. We will show that a is left non-singular in S. Consider the equation $a \circ X = b$, where $b \in S$. Let $\gamma(b) = c \in S'$. Choose $y \in S$ such that $\beta(y) = \alpha(a) \backslash_{\circ'} c$. Then $\alpha(a) \backslash_{\circ'} c$ is the unique solution of the equation $\alpha(a) \circ' Y = c$. Now, it is easy to check that $\beta^{-1}(\alpha(a) \backslash_{\circ'} c)$ is the unique solution of $a \circ X = b$. $\square$

Corollary 2.2. *A right loop isotopic to a loop itself is a loop.*

Let $A = \{a_i | 1 \leq i \leq n\}$ and $B = \{b_i | 1 \leq i \leq n\}$ be sets. We denote the bijective map $\alpha : A \to B$ defined by $\alpha(a_i) = b_i$ as $\alpha = \binom{a_1, a_2, \cdots, a_n}{b_1, b_2, \cdots, b_n}$.

Example 2.3. *Let $G = Sym(3)$ and $H = \{I, (2, 3)\}$, where I is the identity permutation. In this example, we show that $|\mathcal{I}tp(G, H)| = 2$. In this case, $S_1 = \{I, (1, 2, 3), (1, 3, 2)\}$, $S_2 = \{I, (1, 3), (1, 3, 2)\}$, $S_3 = \{I, (1, 3), (1, 2)\}$ and $S_4 = \{I, (1, 2, 3), (1, 2)\}$ are all NRTs of H in G. Since S_1 is loop transversal, by Corollary 2.2 it is not isotopic to S_i $(2 \leq i \leq 4)$. The restriction of $i_{(2,3)}$, the inner conjugation of G by $(2, 3)$, on S_2 is right loop*

isomorphism from S_2 to S_4. One can easily see that $\alpha = \binom{I,(1,3),(1,3,2)}{I,(1,2),(1,3)}$, $\beta = \gamma = \binom{I,(1,3),(1,3,2)}{(1,2),I,(1,3)}$ *is an isotopy from S_2 to S_3. This means that* $|\mathcal{I}tp(G,H)| = 2$.

Proposition 2.4. *Let G be a finite group and H be a subgroup of G. Let $N = Core_G(H)$. Then* $|\mathcal{I}tp(G,H)| = |\mathcal{I}tp(G/N, H/N)|$.

Proof. Let $S \in \mathcal{T}(G,H)$. Clearly $S \mapsto \nu(S) = \{Nx \mid x \in S\}$, where ν is the quotient map from G to G/N, is a surjective map from $\mathcal{T}(G,H)$ to $\mathcal{T}(G/N, H/N)$ such that the corresponding NRTs are isomorphic.

Let $S_1, S_2 \in \mathcal{T}(G,H)$. Let $\delta_1 : S_1 \to \nu(S_1)$ and $\delta_2 : S_2 \to \nu(S_2)$ be isomorphisms defined by $\delta_i(x) = xN$ $(x \in S_i, i = 1,2)$. Assume that (α, β, γ) is an isotopy from S_1 to S_2. Then $(\delta_2\alpha\delta_1^{-1}, \delta_2\beta\delta_1^{-1}, \delta_2\gamma\delta_1^{-1})$ is an isotopy from $\nu(S_1)$ to $\nu(S_2)$. Conversely, if $(\alpha', \beta', \gamma')$ is an isotopy from $\nu(S_1)$ to $\nu(S_2)$, then $(\delta_2^{-1}\alpha'\delta_1, \delta_2^{-1}\beta'\delta_1, \delta_2^{-1}\gamma'\delta_1)$ is an isotopy from S_1 to S_2. Thus $|\mathcal{I}tp(G,H)| = |\mathcal{I}tp(G/N, H/N)|$. $\square$

Remark 2.5. *Let G be a group and H be a non-normal subgroup of G of index 3. Then by Proposition 2.4 and Example 2.3,* $|\mathcal{I}tp(G,H)| = 2$. *The converse of this is false, as we have following example.*

Example 2.6. *Let $G = Alt(4)$, the alternating group of degree 4 and $H = \{I, x = (1,2)(3,4)\}$. In [7, Lemma 2.7, p. 6], we have found that the number of isomorphism classes of NRTs in $\mathcal{T}(G,H)$ is five whose representatives are given by* $S_1 = \{I, z, yz^{-1}, z^{-1}, yz, y\}$, $S_2 = (S_1 \setminus \{yz\}) \cup \{xyz\}$, $S_3 = (S_1 \setminus \{yz, yz^{-1}\}) \cup \{xyz, xyz^{-1}\}$, $S_4 = (S_1 \setminus \{yz^{-1}\}) \cup \{xyz^{-1}\}$ *and* $S_5 = (S_1 \setminus \{z\}) \cup \{xz\}$, *where $z = (1,2,3)$ and $y = (1,3)(2,4)$. We note that S_1 is not isotopic to S_i $(2 \leq i \leq 5)$, for left non-singular elements of S_1 are I, y and z but I, y are those of S_i $(2 \leq i \leq 5)$ (see Proposition 2.1). It can be checked that* $(\alpha_2^j, \beta_2^j, \gamma_2^j)$ $(3 \leq j \leq 5)$ *where* $\alpha_2^3 = \binom{I,z,yz^{-1},z^{-1},xyz,y}{I,z^{-1},xyz,z,xyz,y}$, $\beta_2^3 = \gamma_2^3 = \binom{I,z,yz^{-1},z^{-1},xyz,y}{z,I,xyz^{-1},z^{-1},y,xyz}$; $\alpha_2^4 = \binom{I,z,yz^{-1},z^{-1},xyz,y}{I,yz,z^{-1},xyz^{-1},z,y}$, $\beta_2^4 = \gamma_2^4 = \binom{I,z,yz^{-1},z^{-1},xyz,y}{yz,xyz^{-1},y,I,z^{-1},z}$ *and* $\alpha_2^5 = \binom{I,z,yz^{-1},z^{-1},xyz,y}{I,z,xz^{-1},yz^{-1},yz,y}$, $\beta_2^5 = \gamma_2^5 = \binom{I,z,yz^{-1},z^{-1},xyz,y}{z,xz^{-1},I,y,yz^{-1},yz}$ *is an isotopy from S_2 to S_j.*

Proposition 2.7. *Let G be a finite group and H be a corefree subgroup of G such that* $|\mathcal{I}tp(G,H)| = 1$. *Then*

(i) no $S \in \mathcal{T}(G,H)$ is a loop transversal.

(ii) $\langle S \rangle = G$ *for all* $S \in \mathcal{T}(G, H)$.

Proof. (i) If possible, assume that $T \in \mathcal{T}(G, H)$ is a loop transversal. Then by Corollary 2.2, each $S \in \mathcal{T}(G, H)$ is a loop transversal. By [8, Corollary 2.9, p.74], $H \trianglelefteq G$. This is a contradiction.

(ii) Since $Core_G(H) = \{1\}$, by [3], there exists $T \in \mathcal{T}(G, H)$ such that $\langle T \rangle = G$. This implies $G_T T \cong \langle T \rangle = G$. By the discussion in the second paragraph of this section, $\langle S \rangle = G$ for all $S \in \mathcal{T}(G, H)$. $\square$

Let us recall from [**?**, Introduction, p. 277] that a *free global transversal* S of a subgroup H of a group G is an NRT for all conjugates of H in G. We see from [11, Proposition 4.3.6, p. 103] that a free global transversal is a loop transversal. We now have following:

Proposition 2.8. *Let* G *be a finite nilpotent group and* H *be a subgroup of* G *such that* $|\mathcal{I}tp(G, H)| = 1$. *Then* $H \trianglelefteq G$.

Proof. Let $N = Core_G(H)$. By Proposition 2.4, $|\mathcal{I}tp(G/N, H/N)| = 1$. Now by [**?**, Theorem B, p. 284], there exists a loop transversal of H/N in G/N. This means that each $S \in \mathcal{T}(G, H)$ is a loop transversal (Corollary 2.2). Thus $H/N \trianglelefteq G/N$ ([8, Corollary 2.9, p.74]) and so $H \trianglelefteq G$. $\square$

Proposition 2.9. *Let* G *be a finite solvable group and* H *be a subgroup of* G. *Suppose that the greatest common divisor* $(|H|, [G : H]) = 1$. *Then if* $|\mathcal{I}tp(G, H)| = 1$, *then* $H \trianglelefteq G$.

Proof. Let π be the set of primes dividing $|H|$. Let S be a Hall π'-subgroup of G. Then $S \in \mathcal{T}(G, H)$. Suppose that $|\mathcal{I}tp(G, H)| = 1$. Then by Corollary 2.2 all members of $\mathcal{T}(G, H)$ are loops. Hence by [8, Corollary 2.9, p.74], $H \trianglelefteq G$. $\square$

Corollary 2.10. *Let* G *be a finite group such that* $|G|$ *is a square-free number. Let* $|H|$ *be a subgroup of* G *such that* $|\mathcal{I}tp(G, H)| = 1$. *Then* $H \trianglelefteq G$.

Proof. Since $|G|$ is a square-free number, G is solvable group ([10, Corollary 7.54, p. 197]). Now, the corollary follows from the Proposition 2.9. $\square$

Let $(S, \circ)$ be a right loop. A permutation $\eta : S \to S$ is called a *right pseudo-automorphism*(resp. *left pseudo-automorphism*) if there exists $c \in S$ (resp. left non-singular element $c \in S$) such that $\eta(x \circ y) \circ c = \eta(x) \circ (\eta(y) \circ c)$ (resp. $c \circ \eta(x \circ y) = (c \circ \eta(x)) \circ \eta(y)$) for all $x, y \in S$. The element $c \in S$ is called as *companion* of η. By the same arguement following [5, Lemma 1, p. 215], we record following proposition:

Proposition 2.11. *Let $(S, \circ)$ be a right loop. A permutation $\eta : S \to S$ is right pseudo-automorphism (resp. left pseudo-automorphism) with companiion c if and only if $(\eta, R_c\eta, R_c\eta)$ (resp. $(L_c\eta, \eta, L_c\eta)$) is an autotopy of S. Moreover, if (α, β, γ) is an autotopy on S, then $\alpha(1) = 1 \Leftrightarrow \beta = \gamma \Leftrightarrow \alpha$ is a right pseudo-automorphism with companion $\beta(1)$ (resp. $\beta(1) = 1 \Leftrightarrow \alpha = \gamma \Leftrightarrow \beta$ is a left pseudo-automorphism with companion $\alpha(1)$).*

Let S be a right loop. Denote $A_1(S) = \{(\alpha, \beta, \gamma) \in \mathcal{U}(S) | \alpha(1) = 1\}$ and $A_2(S) = \{(\alpha, \beta, \gamma) \in \mathcal{U}(S) | \beta(1) = 1\}$. It can be checked that $A_1(S)$ and $A_2(S)$ are subgroups of $\mathcal{U}(S)$ and $A_1(S) \cap A_2(S) = Aut(S)$. Since by Proposition 2.1, the left non-singular elements are in bijection for two isotopic right loops, we obtain that [5, Lemma 3, p. 217], [5, Lemma 6, p. 219] and [5, Lemma 8, p. 219] are also true in the case of right loops and can be proved by the same argument used there. Therefore, we also have following extensions of [5, Corollary 7, p. 219] and [5, Corollary 9, p. 220] respectively:

Proposition 2.12. *Let S be a right loop with transitive automorphism group. Then for $i = 1, 2$ either $A_i(S) = Aut(S)$ or the right cosets of $Aut(S)$ in $A_1(S)$ are in one-to-one correspondence with the elements of S and the right cosets of $Aut(S)$ in $A_2(S)$ are in one-to-one correspondence with the left non-singular elements of S.*

Proposition 2.13. *Let S be a right loop with transitive automorphism group. Then for $i = 1, 2$ either $\mathcal{U}(S) = A_i(S)$ or the right cosets of $A_2(S)$ in $\mathcal{U}(S)$ are in one-to-one correspondence with the elements of S and the right cosets of $A_1(S)$ in $\mathcal{U}(S)$ are in one-to-one correspondence with the left non-singular elements of S.*

Now, we have

Theorem 2.14. *Any two isotopic right loops with transitive automorphism groups are isomorphic.*

Proof. Let $(S, \circ)$ be a right loop with transitive automorphism group. Then as remarked in the paragraph 2 of the Section 3, it is enough to prove that, if $a \in S$ is a left non-singular element, $b \in S$ and if $S_{a,b}$ has the transitive automorphism group, then $S \cong S_{a,b}$. So fix $a, b \in S$, where a is a left non-singular element of S. Let $|S| = n$ and m be the number of left non-singular elements in S. In view of Proposition 2.12 and 2.13, we need to consider the following six cases:

Case 1. $[\mathcal{U}(S) : A_1(S)] = 1 = [\mathcal{U}(S) : A_2(S)]$,
Case 2. $[\mathcal{U}(S) : A_1(S)] = m, [\mathcal{U}(S) : A_2(S)] = n, [A_1 : Aut(S)] = 1 = [A_2 : Aut(S)]$,
Case 3. $[\mathcal{U}(S) : A_1(S)] = m, [\mathcal{U}(S) : A_2(S)] = n$, $[A_1(S) : Aut(S)] = n, [A_2(S) : Aut(S)] = m$,
Case 4. $[\mathcal{U}(S) : A_1(S)] = 1, [\mathcal{U}(S) : A_2(S)] = n$, $[A_1(S) : Aut(S)] = n, [A_2(S) : Aut(S)] = 1$,
Case 5. $[\mathcal{U}(S) : A_1(S)] = m, [\mathcal{U}(S) : A_2(S)] = 1$, $[A_1(S) : Aut(S)] = 1, [A_2(S) : Aut(S)] = m$ and
Case 6. $[\mathcal{U}(S) : A_1(S)] = m, [\mathcal{U}(S) : A_2(S)] = 1$, $[A_1(S) : Aut(S)] = 1, [A_2(S) : Aut(S)] = m$.

In each case, the proof is similar to the proof of the corresponding case of [5, Theorem 10, p. 220]. $\square$

Let us now conclude the section by posing some questions:

Question 2.15. *Let G be a finite group and H be a subgroup of G. Does $|\mathcal{I}tp(G, H)| = 1 \Rightarrow H \trianglelefteq G$?*

Question 2.16. *What are the pairs (G, H), where G is a group and H a subgroup of G for which $|\mathcal{I}tp(G, H)| = |\mathcal{I}(G, H)|$, where $|\mathcal{I}(G, H)|$ denotes the isomorphism classes in $\mathcal{T}(G, H)$?*

Question 2.17. *What are the pairs (G, H), where G is a group and H a subgroup of G such that whenever two NRTs in $\mathcal{T}(G, H)$ are isotopic, they are isomophic?*

By Proposition 2.14, we have one answer to the question 3.19 that is the pair (G,H) such that each $S \in \mathcal{T}(G,H)$ has transitive automorphism group.

3 Left non-singular elements in Transversals

The aim of this section is to describe the number of isotopy classes of transversals of a subgroup of order 2 in D_{2p}, the dihedral group of order $2p$, where p is an odd prime.

Let U be a group. Let e denote the identity of the group U. Let $B \subseteq U \setminus \{e\}$ and $\varphi \in Sym(U)$ such that $\varphi(e) = e$. Define an operation $\circ$ on the set U as

$$x \circ y = \begin{cases} xy & \text{if } y \notin B \\ y\varphi(x) & \text{if } y \in B \end{cases} \tag{3.1}$$

It can be checked that $(U, \circ)$ is a right loop. Let us denote this right loop as U_φ^B. If $B = \emptyset$, then U_φ^B is the group U itself. If φ is fixed, then we will drop the subscript φ. Let $\mathbb{Z}_n$ denote the cyclic group of order n. Define a map $\varphi : \mathbb{Z}_n \to \mathbb{Z}_n$ by $\varphi(i) = -i$, where $i \in \mathbb{Z}_n$. Note that φ is a bijection on $\mathbb{Z}_n$. Let $\emptyset \neq B \subseteq \mathbb{Z}_n \setminus \{0\}$. We denote ${\mathbb{Z}_n}_{,\varphi}^B$ by ${\mathbb{Z}_n}^B$. Following lemma describes left non-singuar elements in the right loop ${\mathbb{Z}_n}^B$.

Lemma 3.1. *Let $i \in \mathbb{Z}_n \setminus \{0\}$ (n odd) and $\emptyset \neq B \subseteq \mathbb{Z}_n \setminus \{0\}$. Then i is not a left non-singular in $\mathbb{Z}_n^B$ if and only if the equation $X - Y \equiv i(mod\ n)$ has a solution in $B \times B'$, where X and Y are unknowns and $B' = \mathbb{Z}_n \setminus B$.*

Proof. Let $\circ$ denote the binary operation of $\mathbb{Z}_n^B$. Let $i \in {\mathbb{Z}_n}^B$ such that i is not a left non-singular element. Then for some $x, y \in {\mathbb{Z}_n}^B$ such that $x \neq y$, $i \circ x = i \circ y$. We note that if $x, y \in B$ or $x, y \in B'$, then $i \circ x = i \circ y \Rightarrow x = y$. Therefore, we can assume that $x \in B$ and $y \in B'$. This means that $x - y \equiv 2i(mod\ n)$. Since $j \mapsto 2j$ $(j \in \mathbb{Z}_n)$ is a bijection on $\mathbb{Z}_n$, $x - y \equiv i(mod\ n)$. Thus $X - Y \equiv i(mod\ n)$ has a solution in $B \times B'$.

Conversely, assume that $X - Y \equiv i(mod\ n)$ has a solution in $B \times B'$. Which equivalently implies that, $X - Y \equiv 2i(mod\ n)$ has a solution in $B \times B'$. This means that there exists $(x, y) \in B \times B'$ such that $i \circ x = i \circ y$. Thus, i is not a left non-singular element in ${\mathbb{Z}_n}^B$. $\square$

Proposition 3.2. *Let $n \in \mathbb{N}$ be odd. Then $i \in \mathbb{Z}_n^B$ is a left non-singular if and only if B and B' are unions of cosets of the subgroup $\langle i \rangle$ of the group $\mathbb{Z}_n$. In particular, $i \notin B$.*

Proof. Assume that $i \in \mathbb{Z}_n \setminus \{0\}$ is a left non-singular element. By Lemma 3.1, for no $k \in B'$, $i + k \in B$. This means that $B' = \{i + k | k \in B'\}$. This implies that $\langle i \rangle \subseteq B'$. Therefore, $B' = \cup_{k \in B'}(k + \langle i \rangle)$. As $B \cap B' = \emptyset$, $B = \cup_{k \in B}(k + \langle i \rangle)$.

For the converse, we observe that $B' = \cup_{k \in B'}(k + \langle i \rangle)$ implies that for each $k \in B'$, $i + k \notin B$. Thus by Lemma 3.1, $i \in \mathbb{Z}_n \setminus \{0\}$ is a left non-singular element. □

Corollary 3.3. *If n is an odd prime and $\emptyset \neq B \subseteq \mathbb{Z}_n \setminus \{0\}$, then $0 \in \mathbb{Z}_n^B$ is the only left non-singular element.*

By the similar arguement above, we can record following proposition for even integer n.

Proposition 3.4. *Let $i \in \mathbb{Z}_n \setminus \{0\}$ (n even) and $\emptyset \neq B \subseteq \mathbb{Z}_n \setminus \{0\}$. Then $i \in \mathbb{Z}_n^B$ is a left non-singular if and only if B and B' are unions of cosets of the subgroup $\langle 2i \rangle$ of the group $\mathbb{Z}_n$. In particular, $2i \notin B$.*

Let $G = D_{2n} = \langle x, y | x^2 = y^n = 1, xyx = y^{-1} \rangle$ and $H = \{1, x\}$. Let $N = \langle y \rangle$. Let $\epsilon : N \to H$ be a function with $\epsilon(1) = 1$. Then $T_\epsilon = \{\epsilon(y^i)y^i | 1 \leq i \leq n\} \in \mathcal{T}(G, H)$ and all NRTs $T \in \mathcal{T}(G, H)$ are of this form. Let $B = \{i \in \mathbb{Z}_n | \epsilon(y^i) = x\}$. Since ϵ is completely determined by the subset B, we shall denote T_ϵ by T_B. Clearly, the map $\epsilon(y^i)y^i \mapsto i$ from T_ϵ to $\mathbb{Z}_n^B$ is an isomorphism of right loops. So we may identify the right loop T_B with the right loop ${\mathbb{Z}_n}^B$ by means of the above isomorphism. From now onward, we shall denote the binary operations of T_B as well as of $\mathbb{Z}_n^B$ by $\circ_B$. We observe that $T_\emptyset = N \cong \mathbb{Z}_n$. We obtain following corollaries of Proposition 3.2 and 3.4 respectively.

Corollary 3.5. *Let n be an odd integer. Then there is only one loop transversal in $\mathcal{T}(D_{2n}, H)$.*

Corollary 3.6. *Let n be an even integer. Then there are only two loop transversals in $\mathcal{T}(D_{2n}, H)$.*

Proof. Let $B \subseteq \mathbb{Z}_p \setminus \{0\}$. For $B = \emptyset$, $T_B \cong \mathbb{Z}_n$. Assume that $B \neq \emptyset$. Let $B = \{2i-1 | i \in \mathbb{Z}_n\}$. In this case, $B' = \langle 2 \rangle$ and $B = \langle 2 \rangle + 1$ and $2j \notin B$ for all $j \in \mathbb{Z}_n$. By Proposition 3.4, each $j \in \mathbb{Z}_n^B$ is left non-singular. In this case, $\mathbb{Z}_n^B \cong D_{2(n/2)}$. If $\emptyset \neq B \subsetneqq \{2i-1 | i \in \mathbb{Z}_n\}$, then 1 can not left non-singular element (otherwise $2 \in B'$ and $B' = \{2i | i \in \mathbb{Z}_n\}$). $\square$

Let p be an odd prime. Choose $L \in \mathcal{T}(D_{2p}, H)$, where H is a subgroup of D_{2p} of order 2. Then $L = T_B$ for some $B \subseteq \mathbb{Z}_p \setminus \{0\}$. By Corollary 3.3 and [2, Theorem 1A, p.249], $((R_u^{\circ_B})^{-1}, I, I)$ are the only principal isotopisms from the principal isotope $(L_{0,u}, \circ_u)$ to $(L, \circ_B)$, where $u \in L$, I is the identity map on L and $x \circ_u y = (R_u^{\circ_B})^{-1}(x) \circ_B y$. Let $Aff(1,p) = \{f_{\mu,t} : \mathbb{Z}_p \to \mathbb{Z}_p | f_{\mu,t}(x) = \mu x + t, \text{where } \mu \in \mathrm{Z_p} \setminus \{0\} \text{ and } \mathrm{t} \in \mathrm{Z_p}\}$, *the one dimensional affine group.* For $\emptyset \neq A \subseteq \mathbb{Z}_p \setminus \{0\}$, $\mu \in \mathbb{Z}_p \setminus \{0\}$ and $t \in \mathbb{Z}_p$, let $f_{\mu,t}(A) = \{\mu a + t | a \in A\}$. Let $A' = \mathbb{Z}_p \setminus A$ and $\mathcal{X}_A = \{f_{\mu,u}(A) | u \notin A\} \cup \{(f_{\mu,u}(A))' | u \in A\}$. If $A = \emptyset$, we define $\mathcal{X}_A = \{\emptyset\}$. We have following theorem:

Theorem 3.7. *Let $L = T_B \in \mathcal{T}(D_{2p}, H)$. Then $S \in \mathcal{T}(D_{2p}, H)$ is isotopic to L if and only if $S = T_C$, for some $C \in \mathcal{X}_B$.*

Proof. As observed in the paragraph below the Proposition 3.4 each $S \in \mathcal{T}(D_{2p}, H)$ is of the form T_C and is identified with the right loop $\mathbb{Z}_p^C$ for a unique subset C of $\mathbb{Z}_p \setminus \{0\}$. Thus we need to prove that $\mathbb{Z}_p^C$ is isotopic to $\mathbb{Z}_p^B$ if and only if $C \in \mathcal{X}_B$.

Assume that $B = \emptyset$. Then $L \cong \mathbb{Z}_p$. Since there is exactly one loop transversal in $\mathcal{T}(D_{2p}, H)$ (Corollary 3.5), we are done in this case. Now, assume that $B \neq \emptyset$.

Let $u \in \mathbb{Z}_p \setminus \{0\}$. Let ψ_u and ρ_u be two maps on $\mathbb{Z}_p$ defined by $\psi_u(x) = x + u$ and $\rho_u(x) = u - x$ ($x \in \mathbb{Z}_p$). Note that ${R_u}^{\circ_B} = \psi_u$ or ${R_u}^{\circ_B} = \rho_u$ depending on whether $u \notin B$ or $u \in B$ respectively. First assume that $u \in B$. Then

$$x \circ_u y = \begin{cases} u - x + y & \text{if } y \notin B \\ x + y - u & \text{if } y \in B \end{cases} \tag{3.2}$$

Let $\mu \in \mathbb{Z}_p \setminus \{0\}$. The binary operation $\circ_u$ on L and the map $f_{\mu,u}$ defines a binary operation $\circ_{f_{\mu,u}}$ on $\mathbb{Z}_p$ so that $f_{\mu,u}$ is an isomorphism of right loop from $(\mathbb{Z}_p, \circ_{f_{\mu,u}})$ to $(L_{0,u}, \circ_u)$. We observe that

$$x \circ_{f_{\mu,u}} y = f_{\mu,u}^{-1}(f_{\mu,u}(x) \circ_u f_{\mu,u}(y)) = \begin{cases} x + y & \text{if } y \notin C \\ y - x & \text{if } y \in C, \end{cases} \tag{3.3}$$

where $C = (\mathbb{Z}_p \setminus \{0\}) \setminus f_{\mu,u}^{-1}(B) = \mathbb{Z}_p \setminus f_{\mu,u}^{-1}(B)$. Thus, the right loop $\mathbb{Z}_p$ (with respect to $\circ_{f_{\mu,u}}$) is $\mathbb{Z}_p^{(f_{\mu,u}^{-1}(B))'}$.

Now, assume that $u \notin B$. Then

$$x \circ_u y = \begin{cases} x + y - u & \text{if } y \notin B \\ u - x + y & \text{if } y \in B \end{cases} \tag{3.4}$$

Then above arguments imply that the map $f_{\mu,u}$ is an isomorphism of right loops from $\mathbb{Z}_p^{f_{\mu,u}^{-1}(B)}$ to $L_{0,u}$. Thus $\mathbb{Z}_p^C$ is isotopic to $\mathbb{Z}_p^B$ if $C \in \mathcal{X}_B$.

Conversely, let C be a subset of $\mathbb{Z}_p \setminus \{0\}$ such that $\mathbb{Z}_p^C$ is isotopic to $\mathbb{Z}_p^B$. Let $(\alpha, \beta, \gamma) : \mathbb{Z}_p^C \to \mathbb{Z}_p^B$ be an isotopy which factorizes as $(\alpha, \beta, \gamma) = (\alpha_1, \beta_1, I)(\gamma, \gamma, \gamma)$, where (α_1, β_1, I) is a principal isotopy from a principal isotope L_1 of $\mathbb{Z}_p^B$ to $\mathbb{Z}_p^B$ and an isomorphism γ is an isomorphism from $\mathbb{Z}_p^C$ to L_1. By a description in the second paragraph of Section 3 and by Corollary 3.3, $L_1 = (\mathbb{Z}_p^B)_{0,u}$ for some $u \in \mathbb{Z}_p$ and $\alpha_1 = (R_u^{\circ_B})^{-1}$, $\beta_1 = I$. We have observed that ${R_u}^{\circ_B} = \psi_u$ or ${R_u}^{\circ_B} = \rho_u$ according as $u \notin B$ or $u \in B$ respectively. Then the binary operation on L_1 is given by (4.2). Since γ is an isomorphism from $\mathbb{Z}_p^C$ to L_1,

$$R_y^{\circ_C} = \gamma^{-1} R_{\gamma(y)}^{\circ_u} \gamma \tag{3.5}$$

Assume that $u \in B$. If $\gamma(y) \notin B$, then $R_{\gamma(y)}^{\circ_u} = \rho_{u+\gamma(y)}$ and if $\gamma(y) \in B$, then $R_{\gamma(y)}^{\circ_u} = \psi_{\gamma(y)-u}$. Since conjugate elements have same order, $\gamma^{-1}\rho_{u+\gamma(y)}\gamma = \rho_y$ or $\gamma^{-1}\psi_{\gamma(y)-u}\gamma = \psi_y$ according as $\gamma(y) \notin B$ or $\gamma(y) \in B$ respectively. Further, assume that $\gamma(y) \in B$. Then $\gamma(x+y) = \gamma(x) + \gamma(y) - u$ for all $x, y \in \mathbb{Z}_p$. Observe that $\gamma(0) = u$. By induction, we obtain that

$$\gamma(x) = (\gamma(1) - \gamma(0))x + u. \tag{3.6}$$

Now, assume that $\gamma(y) \notin B$. Then $\gamma(y - x) = \gamma(y) - \gamma(x) + u$, equivalently, $\gamma(x + y) = \gamma(y + x) = \gamma(y) - \gamma(-x) + u$ for all $x, y \in \mathbb{Z}_p$. Observe that $\gamma(0) = u$ and $\gamma(1) + \gamma(-1) = 2u$. By induction, we again obtain that

$$\gamma(x) = (\gamma(1) - \gamma(0))x + u. \tag{3.7}$$

Now, assume that $u \notin B$. Then, by the similar arguments used above we obtain the same formula that in (4.6) and (4.7) for γ.

Since $\gamma(1) \neq \gamma(0)$, we can write $\gamma(x) = \mu x + u$, where $\mu \in \mathbb{Z}_p \setminus \{0\}$ and $u \in \mathbb{Z}_p$. Thus, as argued in the first part of the proof

$$C = \begin{cases} f_{\mu,u}^{-1}(B) & \text{if } u \notin B \\ \mathbb{Z}_p \setminus f_{\mu,u}^{-1}(B) & \text{if } u \in B \end{cases}$$

$\square$

We need following definition for its use in the next theorem :

Let $\mathcal{G}$ denote a permutation group on a finite set X. Let $|X| = m$. For $\sigma \in \mathcal{G}$, let $b_k(\sigma)$ denote the number of k-cycles in the disjoint cycle decomposition of σ. Let $\mathbb{Q}[x_1, \cdots, x_m]$ denote the polynomial ring in indeterminates $x_1, \cdots, x_m$. The *cyclic index* $P_{\mathcal{G}}(x_1, \cdots, x_m) \in \mathbb{Q}[x_1, \cdots, x_m]$ of $\mathcal{G}$ is defined to be

$$P_{\mathcal{G}}(x_1, \cdots, x_m) = \frac{1}{|G|}\Sigma_{\sigma\in\mathcal{G}}\ x_1^{b_1(\sigma)} \cdots x_m^{b_m(\sigma)}$$

(see [4, p. 146]).

Since $\mathbb{Z}_p$ is a vector space over the field $\mathbb{Z}_p$, we get an action of $Aff(1,p)$ on $\mathbb{Z}_p$ and so, it is a permutation group on the set $\mathbb{Z}_p$. Let us calculate the cyclic index $P_{Aff(1,p)}(x_1, \cdots, x_p)$ of $Aff(1,p)$. One can check that the formula we obtain is equal to that in [6, Theorem 3, p. 144].

Lemma 3.8. *The cyclic index of the affine group $Aff(1,p)$ is*

$$P_{Aff(1,p)}(x_1, \cdots, x_p) = \frac{1}{p(p-1)}(x_1^p + p\sum_d \Phi(d)x_1 x_d^{\frac{p-1}{d}} + (p-1)x_p)$$

where the sum runs over the divisors $d \neq 1$ of $p-1$ and Φ is the Euler's phi function.

Proof. We recall that for $\mu \in \mathbb{Z}_p \setminus \{0\}$ and $t \in \mathbb{Z}_p$, $f_{\mu,t} \in Aff(1,p)$ defined by $f_{\mu,t}(x) = \mu x + t$. We divide the members of $Aff(1,p)$ into following three disjiont sets

(a) $C_0 = \{I = \text{the identity map on } \mathbb{Z}_\mathrm{p}\}$

(b) $C_1 = \{f_{\mu,t} | \mu \in \mathbb{Z}_p \setminus \{0\}, \mu \neq 1, t \in \mathbb{Z}_p\}$

(c) $C_2 = \{f_{1,t} | t \in \mathbb{Z}_p \setminus \{0\}\}$

There are $p(p-2)$ elements in the set C_1. By [6, Lemma 2, p. 143], we note that if $\mu \in \mathbb{Z}_p \setminus \{0\}, \mu \neq 1, t \in \mathbb{Z}_p$, then $f_{\mu,t}$ and $f_{\mu,0}$ has same cycle type. We note that $K = \{f_{\mu,0} | \mu \in \mathbb{Z}_p \setminus \{0\}\} \cong \mathbb{Z}_{p-1}$ and if $f_{\mu,0} \in K$ is of order l, then $f_{\mu,0}$ is a product of $\frac{p-1}{l}$ disjoint cycles of length l and there are $\Phi(l)$ such permutations in K of order l. Also, each element in the set C_1 fixes

exactly one element. Order of each element in the set C_2 is p and there are $p-1$ such elements. Thus, we obtain the cyclic index of $Aff(1,p)$ to be

$$\frac{1}{p(p-1)}(x_1^p + p\sum_d \Phi(d)x_1 x_d^{\frac{p-1}{d}} + (p-1)x_p)$$

$\square$

Theorem 3.9. *Let D_{2p} denote the finite dihedral group (p an odd prime) and H be a subgroup of order 2. Then $|\mathcal{I}tp(D_{2p}, H)| = \frac{P_{Aff(1,p)}(2,\cdots,2)}{2}$.*

Proof. By the Theorem 3.7, we see that the set $\mathcal{X}_B$ ($B \subseteq \mathbb{Z}_p \setminus \{0\}$) determines the isotopy classes in $\mathcal{T}(D_{2p}, H)$. This means that $|\mathcal{I}tp(D_{2p}, H)| = |\{\mathcal{X}_B | B \subseteq \mathbb{Z}_p \setminus \{0\}\}|$. The action of $Aff(1,p)$ on $\mathbb{Z}_p$ induces an action $'*'$ of $Aff(1,p)$ on the power set of $\mathbb{Z}_p$. This action preserves the size of each subset of $\mathbb{Z}_p$. We note that two subsets A and B of same size are in the same orbit of the action $*$ if and only if $B = \mu A + j$ for some $\mu \in \mathbb{Z}_p \setminus \{0\}$ and $j \in Z_p$. We observe that for a non-empty subset B of $\mathbb{Z}_p \setminus \{0\}$, $\mathcal{X}_B$ contains the sets of size $|B|$ as well as of size $p - |B|$. This means that it is sufficient to describe $\mathcal{X}_B$ by the set B such that $|B| \leq \frac{p-1}{2}$. Therefore, by [4, Theorem 5.1, p. 157; Example 5.18, p.160] and Lemma 3.8, we see that $|\mathcal{I}tp(D_{2p}, H)| = |\{\mathcal{X}_B | B \subseteq D_{2p}\}| = \frac{P_{Aff(1,p)}(2,\cdots,2)}{2}$. $\square$

Example 3.10. *We list $|\mathcal{I}tp(D_{2p}, H)|$ for $p = 3, 5, 7$, where H is subgroup of D_{2p} of order 2.*

1. $|\mathcal{I}tp(D_6, H)| = 2$. *We have already calculated this in Example 2.3.*

2. $|\mathcal{I}tp(D_{10}, H)| = 3$.

3. $|\mathcal{I}tp(D_{14}, H)| = 5$.

References

[1] R. H. Bruck, Some results in the theory of linear non-associative algebras, *Trans. Amer. Math. Soc.* **56**, (1944), 141199.

[2] R. H. Bruck, Contributions to the Theory of Loops, *Tran. A. M. S. Vol.*, **60(2)**, (1946), 245-354.

[3] Cameron, P. J., *http://maths.qmul.ac.uk/pjc/preprints/transgenic.pdf*

[4] N.G. de Bruijn, Polya's theory of counting. In E.F. Beckenbach, editor, *Applied Combinatorial Mathematics*, chapter 5, John Wiley & Sons, Inc., 1964, 144184.

[5] A. A. Drisko, Loops with Transitive Automorphisms, *J. Algebra*, **184**, (1996), 213-239.

[6] H. Fripertinger, Cyclic Indices of Linear, Affine, and Projective Groups, *Linear Algebra Appl.*, **263**, (1997), 133-156 .

[7] Vipul Kakkar, R. P. Shukla, On the Number of Isomorphism Classes of Transversals, To appear in *Proc. Indian Acad. Sci. (Math. Sci.).*

[8] R. Lal, Transversals in Groups, *J. Algebra*, **181**, (1996), 70-81.

[9] R. Lal and R. P. Shukla, Perfectly stable subgroups of finite groups, *Comm. Algebra*, **24(2)**, (1996), 643-657.

[10] J. J. Rotman, *An Introduction to the Theory of Groups*, Springer-Verlag New York, Inc., 1995.

[11] J. D. H. Smith and Anna B. Romanowska, *Post-Modern Algebra*, John Wiley & Sons, Inc., 1999.

[12] H. Zassenhaus, *The Theory of Groups*, Chelsea, New York, 1949.